

DEPARTMENT OF STATE
PRIVACY IMPACT ASSESSMENT
FISCAL YEAR 2008
Personnel Reporting and Statistics
(PRAS)

Conducted by:
Bureau of Administration
Information Sharing Services
Office of Information Programs and Services
Privacy (PRV)
Email: pia@state.gov

A. SYSTEM APPLICATION/GENERAL INFORMATION:

- 1) Does this system contain any personal information about individuals or *personally identifiable information? If the answer is no, please reply via e-mail to the following e-mail address at pia@state.gov If the answer is yes, please complete the survey in its entirety.**
YES X NO

*The following are examples of personally identifiable information:

- Name of an individual
- Date and place of birth
- Address
- Telephone number
- Social security, Passport, Driver's license or other identifying number(s)
- Education
- Financial transactions
- Employment, Medical or Criminal history
- Finger print, voice print or photograph
- Any other identifying attribute assigned to the individual

2) What is the purpose of the system/application?

The Personnel Reporting and Statistics (PRAS) system is a standalone network that supports the official human resources data reporting and analysis requirements of both the Bureau of Human Resources and the Department of State. PRAS information includes month-end employee/position data downloaded from the Global Employee Management System (GEMS) and from the Internal Data Broker (IDB) by way of the HR Bureau's Knowledge Center (KC). No "personally identifiable information" is modified directly in PRAS. In addition, there are some PRAS specific data elements (or derived variables) that are created solely for the purposes of simplifying the reporting process.

Note: GEMS and/or IDB contain the following types of employee and position data:

1) Personal data includes name, social security number, address, sex, citizenship, date and place birth, marital status, and the names and birth dates of eligible family members; 2) Career data includes education level, college(s) attended, major subjects, skill codes, foreign language training and examination scores; 3) Job history data includes both current and previous position titles, pay plans, grades, assignment dates, locations, and pending assignment information; and 4) Organizational data includes organizational hierarchies, accounting information, awards, disciplinary actions, etc.

3) What legal authority authorizes the purchase or development of this system/application?

C. DATA IN THE SYSTEM:

1) Does a Privacy Act system of records already exist?

YES X NO

If yes, please provide the following:

System Name: Human Resources Records **Number:** State-31

If no, a Privacy system of records description will need to be created for this data.

2) What categories of individuals are covered in the system?

All Department of State Civil Service and Foreign Service direct hire employees, including Foreign Service Consular Agents.

3) What are the sources of the information in the system?

a. Is the source of the information from the individual or is it taken from another source? If not directly from the individual, then what other source?

The source of monthly PRAS system data comes from GEMS and IFSAMA through a monthly download from the HR Bureau's Knowledge Center. In addition, historical month-end snapshots of mainframe (pre-GEMS) personnel data has been converted into PRAS for select data elements going back to the late 1970s.

Note: In GEMS, the individual provides all initial information through the submittal of a resume, SF-171, OF-612, or other equivalent employment forms (locator info, check-in forms, assignment cables, etc.). Department-sponsored training data, including language training, is provided by the Foreign Service Institute's Student Training Management System (STMS). Payroll related information is provided by the Bureau of Resource Management's Consolidated American Payroll and Pension System (CAPPS).

b. Why is the information not being obtained directly from the individual?

PRAS is designed as a reporting mechanism only. No employee specific data is directly updated in PRAS.

c. What Federal agencies are providing data for use in the system?

None.

d. What State and/or local agencies are providing data for use in the system?

None.

e. From what other third party sources will data be collected?

None.

f. What information will be collected from a State Department employee and the public?

As stated above, the Knowledge Center contains GEMS/IFSAMA data and is the exclusive provider of PRAS information. No personal data is collected for PRAS directly from a Department employee or the public.

Note: In GEMS, personal information, such as SSN, date of birth, race and national origin, marital status, dependents, education, etc., is collected from the employee. Public information is not collected for GEMS or IFSAMA.

4) Accuracy, Timeliness, and Reliability

a. How will data collected from sources other than DOS records be verified for accuracy?

All PRAS data is collected from Department of State records and is validated by the source applications (GEMS/IFSAMA) using edit checks for permitted values.

Note: In GEMS, the human resources management specialist will manually verify employee data contained in the official personnel folder (OPF) against Form SF-75 information provided by other Federal agencies. In addition, GEMS data is validated by output reports and quality reviews.

b. How will data be checked for completeness?

PRAS data is dependent on the GEMS/IFSAMA applications to enforce data integrity and completeness through the use of edits, permitted values, internal management reports and quality reviews.

- c. Is the data current? What steps or procedures are taken to ensure the data is current and not out-of-date? Name the document (e.g., data models).**

PRAS data is current as of the last day of the preceding month. At most, PRAS data is 30 days old and currency is dependent upon GEMS/IFSAMA source system edits, internal management reports and quality reviews.

- d. Are the data elements described in detail and documented? If yes, what is the name of the document?**

Yes, most PRAS data elements are described in the GEMS Data Dictionary, OPM's Guide to Data Standards, and 3 FAM 2340, *Personnel Actions* (currently being revised).

D. DATA CHARACTERISTICS:

- 1) Is the use of the data both relevant and necessary to the purpose for which the system is being designed?**

Yes.

- 2) Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected, and how will this be maintained and filed?**

Yes. PRAS incorporates derived variable data elements that aggregate data for easier reporting. For instance, derived variables are used to identify groups of employees (e.g., FS Generalists, FS Specialists, etc.) so that the PRAS user can easily create a report without having to remember business logic used to determine this information.

- 3) Will the new data be placed in the individual's record?**

No. The derived information in PRAS is specific to aggregate reporting and will not appear in the individual's record.

4) Can the system make determinations about employees/public that would not be possible without the new data?

No. Although derived information exists in PRAS, it is used mostly for aggregate reporting purposes. For instance, PRAS may contain derived information to identify a group of employees who are eligible to retire as of a specific date but it can't determine who/when of those employees will actually retire.

5) How will the new data be verified for relevance and accuracy?

Derived information will be verified through internal application edits and data quality checks.

6) If the data is being consolidated, what controls are in place to protect the data from unauthorized access or use?

PRAS is a stand alone network that incorporates physical, network, and application security controls. As an isolated network, PRAS does not connect to any other system or network and only authorized users have access.

7) If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.

The same procedures are applied to the consolidation of processes as indicated in question 6 above.

8) How will the data be retrieved? Does a personal identifier retrieve the data? If yes, explain and list the identifiers that will be used to retrieve information on the individual.

Data can be retrieved using any field in the PRAS application. Department employees are uniquely identified by social security numbers (SSNs) or GEMS Employee ID. Authorized PRAS users are issued user Ids and passwords in accordance with Department guidelines published in the 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*.

9) What kinds of reports can be produced on individuals? What will be the use of these reports? Who will have access to them?

PRAS is intended to support standard aggregate reporting for statistical analysis, trend analysis, skills inventories, data quality reviews, internal management controls, and official reporting both inside and outside of the Department. PRAS users also create ad-hoc reports, reflecting individual employee information, to further identify data quality errors discovered through standard reporting. These ad-hoc reports are disseminated to the appropriate offices for data correction in the source system.

E. MAINTENANCE AND ADMINISTRATIVE CONTROLS:

1) If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?

PRAS is a stand-alone network and all servers are located in Washington, DC (State Annex-1). All data is stored and maintained centrally.

2) What are the retention periods of data in this system?

All PRAS electronic data is retained using the same disposition schedule as GEMS.

Note: In accordance with System 31, GEMS electronic data is maintained until it becomes inactive, at which time it will be retired or destroyed in accordance with published record schedules of the Department of State and as approved by the National Archives and Records Administration (NARA). The retention schedule for the data stored in GEMS is currently with NARA for review and approval. The proposed disposition of magnetic tape and CD-ROM storage mediums is permanent with transfer to the NARA when 30 years old or sooner, if negotiated with NARA.

3) What are the procedures for disposition of the data at the end of the retention period? How long will the reports produced be kept? Where are the procedures documented?

All PRAS electronic data is retained using the same disposition schedule as GEMS.

Note: GEMS record disposition procedures are provided in State-31 and in accordance with the 5 Foreign Affairs Handbook (FAH)-4, Records Management Handbook.

4) Is the system using technologies in ways that the DOS has not previously employed (e.g., monitoring software, Smart Cards, Caller-ID)?

Not at present. However, smart cards and other monitoring technologies are planned for future use.

5) How does the use of this technology affect public/employee privacy?

Use of the system and its technology does not affect public/employee privacy.

6) Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.

Yes.

Identification: PRAS stores personal data such as SSNs, citizenship, sex, and dates of birth that may be used for identification purposes.

Locate: PRAS stores the employee's official duty station and organization to which assigned.

Monitor: As previously stated, no data is updated directly in PRAS. In addition, the PRAS network provides the capability for monitoring user access.

7) What kinds of information are collected as a function of the monitoring of individuals?

PRAS network user names, user IDs, etc., are collected for recording individuals' logon dates and times.

8) What controls will be used to prevent unauthorized monitoring?

See response to Section D6.

9) If the system is being modified, will the Privacy Act system of records notice require amendment or revision? Explain.

No. However, most PRAS source data comes from GEMS/IFSAMA and State-31 will be revised if/when GEMS/IFSAMA system modifications affect employee information protected under the Privacy Act of 1974, as amended.

10) Are there forms associated with the system? YES X NO
If yes, do the forms include Privacy Act statements that include required information (e.g. – legal authorities allowing for the collection of the information being requested, whether provision of the information is mandatory or voluntary, the routine uses of the data, with whom the data will be shared, the effects on the individual if the data is not provided)?

A Privacy Act statement is included on all HR system access request forms including the following: 1) Request for HR Systems Access; and 2) Request to Revise Access for Active Operator.

F. ACCESS TO DATA:

1) Who will have access to the data in the system (e.g., contractors, users, managers, system administrators, developers, other)?

Department employee users, contractors, managers, and system administrators have access to data in PRAS.

2) How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?

The user and the user's immediate supervisor determine access to PRAS. If the user is a contractor they must obtain the approval of their respective contracting officer technical representative (COTR), the PRAS system manager and the PRAS program manager. There are two forms used to request access to PRAS: 1) Request for HR Systems Access; and 2) Request to Revise Access for Active Operator.

3) Will users have access to all data on the system or will the user's access be restricted? Explain.

Data access is restricted in PRAS based on user requirement. Network access is limited to the user's role and/or folder depending upon user type (e.g., user, developer, system administrator, etc.). Additional network controls further restrict PRAS access to the user's workstation.

4) What controls are in place to prevent the misuse (e.g., unauthorized browsing) of data by those having access? (Please list processes and training materials)

Users are required to read and sign the Users Certification Statement on the Request for HR Systems Access form. The statement informs the user that accessing the system for purposes outside the scope of authorization constitutes a violation of Federal Law (18 U.S. C. & 130, et al, the Privacy Act).

Internal network monitoring, auditing and management reports further prohibit unauthorized use.

5) Are contractors involved with the design and development of the system and will they be involved with the maintenance of the system? If yes, were Privacy Act contract clauses inserted in their contracts and other regulatory measures addressed? Have rules of conduct been established and training regarding the handling of such information under the Privacy Act of 1974, as amended?

Yes, contractors design, develop and maintain the system. Privacy Act clauses are present in the contracts and in the statements of work (SOW). All contractor personnel are required to pass a National Agency Check prior to being assigned to work on the contract. In addition, all contractors have to acknowledge the Privacy Act clause contained on the Request for HR Systems Access.

6) Do other systems share data or have access to the data in the system? If yes, explain.

No. GEMS and IFSAMA source data in the Knowledge Center is downloaded into PRAS on a monthly basis for reporting purposes only. PRAS data is not shared with any other application or system.

7) Who will be responsible for protecting the privacy rights of the public and employees affected by the interface?

Each application system owner is responsible for protecting privacy rights.

8) Will other agencies share data or have access to the data in this system (Federal, State, Local, Other)?

No. As mentioned in #6 above, PRAS does not share data with any other application either internal or external to the Department of State.

9) If so, how will the data be used by the other agency?

Not applicable. See #8 above.

10) Who is responsible for assuring proper use of the data?

The Director General of the Foreign Service and Director of Personnel.